Explicit Bounds for the Burgess Inequality for Character Sums

Enrique Treviño

INTEGERS, October 16, 2009

Dirichlet Characters

Definition (Character)

A character χ is a homomorphism from a finite abelian group G to $\mathbb{C}^*$.

Definition (Dirichlet Character)

Dirichlet characters of modulus n are characters over the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$ and extend it to $\mathbb{Z}$ by having $chi(m) = m \pmod{n}$ if $(m, n) = 1$ and $\chi(m) = 0$ if and only if $(m, n) > 1$.

- $\chi(m) = 1$ for all $(m, n) = 1$. Called the principal character.
- For modulus p prime, let $\chi(m) = \left(\frac{m}{p}\right)$, the Legendre symbol.

Short Character Sums, Why bother?

I will be interested in short character sums. If we let χ be a non-principal character of modulus p then a short character sum looks like this:

$$S_\chi(N) = \sum_{M<n\leq N+M} \chi(n)$$

Applications:

- Improving upperbound for least quadratic non-residue (mod p)
- Calculating $L(1, \chi)$

Polya-Vinogradov

Theorem (Polya-Vinogradov)

For χ a non-principal Dirichlet character to the modulus q

$$S_\chi(N) \ll \sqrt{q} \log q$$

Constant made explicit and improved by people over time.

Theorem (Pomerance)

If χ is a non-principal Dirichlet character to the modulus q, where $q \geq 500$ then

$$S_\chi(N) \leq \frac{1}{3 \log 3} \sqrt{q} \log q + 2\sqrt{q}$$

Burgess

In the 60s, Burgess came out with the following:

Theorem (D. Burgess)

Let χ be a primitive character of conductor $q > 1$. Then

$$S_\chi(N) = \sum_{M < n \le M+N} \chi(n) \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon}$$

for $r = 2, 3$ and for any $r \ge 1$ if q is cubefree, the implied constant depending only on ϵ and r.

Explicit Constants

Theorem (Iwaniec-Kowalski-Friedlander)

Let χ be a Dirichlet character mod p. Then for $r \geq 2$

$$|S_\chi(N)| \leq 30 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Improvement

Theorem (ET)

Let χ be a Dirichlet character mod p. Then for $r \geq 2$ and $p \geq 10^7$.

$$|S_\chi(N)| \leq 3 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Note, the constant gets better for larger r, for example for $r = 3, 4, 5, 6$ the constant is $2.376, 2.085, 1.909, 1.792$ respectively.

Proof

Idea 1: Shift, take average and use induction

$$S_\chi(N) = \sum_{M<n\leq M+N} \chi(n+ab) + \sum_{M<n\leq M+ab} \chi(n) - \sum_{M+N<n\leq M+N+ab} \chi(n)$$

$1 \leq a \leq A$, $1 \leq b \leq B$.
Take average as a and b move around their options.

Proof Cont.

$$V = \sum_{a,b} \sum_{M<n\leq M+N} \chi(n+ab)$$

Since $\chi(n+ab) = \chi(a)\chi(\bar{a}n+b)$, we have that

$$V = \sum_{x \pmod p} v(x) \left| \sum_{1\leq b\leq B} \chi(x+b) \right|$$

where $v(x)$ is the number of ways of writing x as $\bar{a}n$ where a and n are in the proper ranges.

Proof Cont.

Idea 2: Holder's Inequality

- Let $V_1 = \sum_{x \pmod p} v(x) = AN$
- Let $V_2 = \sum_{x \pmod p} v^2(x)$
- Let $W = \sum_{x \pmod p} \left| \sum_{1 \leq b \leq B} \chi(x+b) \right|^{2r}$.

By Holder's Inequality we get

$$V \leq V_1^{1-\frac{1}{r}} V_2^{\frac{1}{2r}} W^{\frac{1}{2r}}$$

Proof Cont.

Lemma

For $A \geq 40$ *and* $A \leq \frac{N}{15}$,

$$V_2 = \sum_{x \pmod p} v^2(x) \leq 2AN\left(\frac{AN}{p} + \log(2A)\right)$$

V_2 is the number of quadruples (a_1, a_2, n_1, n_2) with $1 \leq a_1, a_2 \leq A$ and $M < n_1, n_2 \leq M + N$ such that $a_1 n_2 \equiv a_2 n_1 \pmod p$.

$$V_2 \leq AN + 2\sum_{a_1 < a_2}\left(\frac{(a_1 + a_2)N}{\gcd(a_1, a_2)p} + 1\right)\left(\frac{\gcd(a_1, a_2)N}{max\{a_1, a_2\}} + 1\right)$$

Heart of the proof

Lemma

$$W = \sum_{x \pmod p} \left| \sum_{1 \le b \le B} \chi(x+b) \right|^{2r} \le r^{2r} B^r p + (2r-1) B^{2r} \sqrt{p}$$

$$W = \sum_{x \pmod p} \left| \sum_{1 \le b \le B} \chi(x+b) \right|^{2r} = \sum_{b_1, \ldots, b_{2r}} \sum_{x \pmod p} \chi\left(\frac{(x+b_1)\ldots(x+b_r)}{(x+b_{r+1})\ldots(x+b_{2r})} \right).$$

Letting $f(x)$ be the function inside χ, we can use Weil's theorem (Riemann Hypothesis on Curves) to bound it by $\sqrt{p}$ if $f(x)$ is not a k-th power where k is the order of χ.

By using Weil's theorem when $f(x)$ is a k-th power and using the trivial bound of p whenever $f(x)$ is not a k-th power we can estime W to get the lemma.

Ending the Proof

- Optimize choice of A and B.
- Use inductive hypothesis to bound the sums of length AB.
- Put it all together and compute.

Quadratic Case (Booker)

Theorem (Booker)

Let $p > 10^{20}$ be a prime number $\equiv 1 \pmod 4$, $r \in \{2, \ldots, 15\}$ and $0 < M, N \le 2\sqrt{p}$. Let χ be a quadratic character $\pmod p$. Then

$$\left| \sum_{M \le n < M+N} \chi(n) \right| \le \alpha(r) p^{\frac{r+1}{4r^2}} (\log p + \beta(r))^{\frac{1}{2r}} N^{1-\frac{1}{r}}$$

where $\alpha(r), \beta(r)$ are given by

r	$\alpha(r)$	$\beta(r)$	r	$\alpha(r)$	$\beta(r)$
2	1.8221	8.9077	9	1.4548	0.0085
3	1.8000	5.3948	10	1.4231	-0.4106
4	1.7263	3.6658	11	1.3958	-0.7848
5	1.6526	2.5405	12	1.3721	-1.1232
6	1.5892	1.7059	13	1.3512	-1.4323
7	1.5363	1.0405	14	1.3328	-1.7169
8	1.4921	0.4856	15	1.3164	-1.9808

Improving the range

For $r \geq 3$ we can do the following:

$$c_r N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} \log(p)^{\frac{1}{2r}} < c_2 N^{\frac{1}{2}} p^{\frac{3}{16}} \log(p)^{\frac{1}{2}}$$

Then

$$N \leq \left(\frac{c_2}{c_r}\right)^{\frac{2r}{r-2}} p^{\frac{3r+2}{8r}} (\log(p))^{\frac{r-1}{r-2}}$$

Therefore we have $N < \sqrt{p}$. Hence the range Booker gets can be extended for $r \geq 3$.

Improving the Log Factor in the General Case

The same trick gets us to improve my theorem to:

Theorem (ET)

Let χ be a Dirichlet character mod p. Then for $r \geq 3$

$$|S_\chi(N)| \leq 3.1 \cdot N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p + 6)^{\frac{1}{2r}}.$$

Acknowledgements

- My advisor Carl Pomerance for suggesting the problem and guidance.
- Burgess, Iwaniec, Friedlander, Kowalski, Booker, Montgomery, Vaughan, and Granville for their work on short character sums.